UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/784,700	02/23/2004	Tsuneki Takahashi	1990.69815	1323

7590 04/03/2009

Patrick G. Burns, Esq.
GREER, BURNS & CRAIN, LTD.
Suite 2500
300 South Wacker Dr.
Chicago, IL 60606

EXAMINER	
OKORONKWO, CHINWENDU C	
ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
04/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/784,700	TAKAHASHI, TSUNEKI	
	Examiner	Art Unit	
	CHINWENDU C. OKORONKWO	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4 and 6-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4 and 6-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *Multiple (20090217)*.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. In response to communications filed on 12/31/2008, the Examiner acknowledges the amendments made to the claims and have both considered and applied them to the claims.

Response to Remarks/Arguments

2. Applicant's arguments with respect to the rejection of claims1-15 have been fully considered but they are not persuasive.

Note that although the Examiner responds to some of the arguments below, the Examiner has further countered particular arguments with an additional reference, so as to fully establish the position of the Examiner regarding the claimed and argued limitations.

2.1 In response to Applicant argument that the Sako reference does not teach or suggest a magnetic disk apparatus that includes a cipher key change unit which changes the cipher key used for decoding the data stored in the record medium, in addition to the previous citation the Examiner respectfully disagrees, citing Figure 1 and paragraph 0028 – "cipher key data is ... data based on serial number etc. of the recording medium 16 on which to record the contents data." The recording medium is equated to the claimed "magnetic disk apparatus" and cipher key data is equated to the claimed "cipher key."

2.2 In response to Applicant argument that the Sako reference does not teach or suggest erasing a first cipher key stored in a cipher key memory unit, in addition to the previous citation the Examiner respectfully disagrees, citing the newly included reference, Montgomery et al. (US Patent No. 7,392,404 *hereinafter* Montgomery), and Figure 1 and paragraph 0028 of the current reference, Sako, which recites, "when the second switching circuit 28 is off and then first switching circuit 27 is on, the encryption circuit 15 is supplied with compressed contents data deciphered by the deciphering circuit 12. The encryption circuit 15 encrypts compressed data, supplied thereto with cipher key data distinct from the cipher key data of the contents data supplied." The Examiner understands the disclosed encryption circuit using "cipher key data distinct" or different "from the cipher key data of the contents data" to encrypt compressed data due to the switching circuit setting reads upon the claimed and argued "cipher key change step of changing the cipher key that corresponds to stored data and that is used in the encoding/recording step." The obviousness-type reasoning is provided below within the rejection.

2.3 In response to Applicant argument that the Sako reference does not teach or suggest a second cipher key that "cannot decode the encoded data recorded on the disk medium," the Examiner respectfully disagrees, citing (in addition to the previous citations) paragraph 0028 which recites an "encryption circuit [that] uses cipher key data distinct from the cipher key data used for the contents data supplied to the input terminal 11, or uses a distinct cipher system, to improve the safety of the contents data."

2.4 In response to Applicant argument that the Sako reference does not teach or suggest "in response to a command for discarding all of a first encoded data recorded on the medium," the Examiner respectfully disagrees, column 7 lines 12-21 of the newly included reference, Montgomery, which recites, "in one embodiment of the present invention, executing a tamper protocol (block 740) may erase the key to decode data stored in memory" and paragraph 0026-0027 of the current reference, Sako, which recites, "The detection circuit 26 receives the contents data, decoded in the deciphering circuit 12 and decompressed in the decompression circuit 13. From the input contents data, the detection circuit 26 extracts watermark signals from a critical band on the frequency axis or on the time axis and decodes the so extracted watermark signals to generate copyright management data. The detection circuit 26 outputs the copyright management data to the recording controlling circuit 23, while controlling the switching of the first and second switching circuits 27, 28 based on the copyright management data. Specifically, when copyright management data, generated from the extracted watermark signals, permit recording of the contents data, the detection circuit 26 changes over the state of one of the first and second switching circuits 27, 28 to an on-state to permit the recording of the contents data on the recording medium 16. Conversely, when the copyright management data, generated from the extracted watermark signals, inhibit recording of the contents data, the detection circuit 26 changes over the states of both the first and second switching circuits 27, 28 to an off-

state to inhibit the recording of the contents data on the recording medium 16." The obviousness-type reasoning is provided below within the rejection.

2.5 In response to Applicant argument that the Sako reference does not teach or suggest "discarding all of a first encoded data recorded on a magnetic disk medium," the Examiner respectfully disagrees again citing (in addition to the previous citations) , citing column 7 lines 12-21 of the newly included reference, Montgomery, which recites, "in one embodiment of the present invention, executing a tamper protocol (block 740) may erase the key to decode data stored in memory" and paragraph 0026-0027 of the current reference, Sako, which recites, "The detection circuit 26 receives the contents data, decoded in the deciphering circuit 12 and decompressed in the decompression circuit 13. From the input contents data, the detection circuit 26 extracts watermark signals from a critical band on the frequency axis or on the time axis and decodes the so extracted watermark signals to generate copyright management data. The detection circuit 26 outputs the copyright management data to the recording controlling circuit 23, while controlling the switching of the first and second switching circuits 27, 28 based on the copyright management data. Specifically, when copyright management data, generated from the extracted watermark signals, permit recording of the contents data, the detection circuit 26 changes over the state of one of the first and second switching circuits 27, 28 to an on-state to permit the recording of the contents data on the recording medium 16. Conversely, when the copyright management data, generated from the extracted watermark signals, inhibit recording of the contents data,

the detection circuit 26 changes over the states of both the first and second switching circuits 27, 28 to an off-state to inhibit the recording of the contents data on the recording medium 16." The Examiner understands the data outputted by the detection circuit 26 to the recording controlling circuit 23, which results in controlling or effecting a change or maintenance to the setting(s) of switching circuits 27 and 28 which is a circuit responsible for determining if the cipher key data will be changed or not. Therefore, it is understood by the Examiner that the copyright management data output by the detection circuit 26 will function as a command for the switching circuits 27 and 28 which can subsequently change the cipher key data, as this data will either "permit recording of the contents data, the detection circuit 26 changes over the state of one of the first and second switching circuits 27, 28 to an on-state to permit the recording of the contents data on the recording medium 16 ... [or] conversely when the copyright management data, generated from the extracted watermark signals inhibit[s] recording of the contents data, the detection circuit 26 changes over the states of both the first and second switching circuits 27, 28 to an off-state to inhibit the recording of the contents data on the recording medium 16 (0026)." The obviousness-type reasoning is provided below within the rejection.

2.6 In response to Applicant argument that the Sako reference does not teach or suggest making "decoding the first encoded data impossible," the Examiner respectfully disagrees citing paragraph 0028 which recites an "encryption circuit [that] uses cipher key data distinct from the cipher key data used for the contents data supplied to the

input terminal 11, or uses a distinct cipher system, to improve the safety of the contents data." It is understood that with the distinct cipher system disclosed here, it would indeed be impossible to decode the contents data with the original cipher key data.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4 and 6-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sako et al. (US Patent Application Publication No. 20040131183 A1) and further in view of Montgomery et al. (US Patent No. 7,392,404 *hereinafter* Montgomery).

Regarding claim 1, Sako et al., provides an obvious type disclosure of a magnetic disk apparatus comprising:

- a cipher key memory unit which stores a single cipher key used for encoding and decoding data (Figure 1, 0023, 0028 and 0031 – "deciphering circuit 12 is supplied with encrypted encoded contents data transmitted to the input terminal 11 from another device, or which is read out from a recording medium, such as an optical disc.

The deciphering circuit 12 has stored in an internal memory, not shown, compressed encrypted contents data for deciphering the contents data and, when the compressed encrypted contents data are supplied from the input terminal 11, deciphers the contents data, using cipher key data stored in a memory. The deciphering circuit 12 outputs the decoded compressed data to the decompression circuit 13 and to the first selector 21," "encryption circuit 15 is supplied with compressed contents data deciphered by the deciphering circuit 12. The encryption circuit 15 encrypts compressed data, supplied thereto with cipher key data distinct from the cipher key data of the contents data supplied" and "encryption circuit 18 receives contents data compressed by the compression circuit 17. The encryption circuit 18 has stored cipher key data in an internal memory, not shown, and encrypts the input contents data using the cipher key data read out from this memory.");

- a cipher encode unit which encodes data input via an interface from an upper apparatus using the cipher key stored in said cipher key memory unit, the cipher encode unit recording the encoded data onto a magnetic disk medium (0007-0011 and 0023-0028);
- a cipher decode unit which decodes the encoded data read out from the magnetic disk medium using the cipher key stored in said

cipher key memory unit, the cipher decode unit outputting the decoded data via the interface to the upper apparatus (0007-0011 and 0023-0028);

- cipher key stored in said cipher key memory unit, defined as a first cipher key, and replaces the first cipher key with another key, defined as a second cipher key, which cannot decode the encoded data recorded on the magnetic disk medium (0007-0011 and 0023-0028); and
- wherein the cipher key change unit replaces the first cipher key stored in said cipher key memory unit with the second cipher key in response to a command for discarding all of a first encoded data recorded on the magnetic disk medium, and makes decoding the first encoded data impossible, the first encoded data encodes using the first cipher key stored in said cipher key memory unit (0007-0011 and 0023-0028).

Although Sako does not explicitly disclose both the cipher keys used for encryption and decryption, it would have been obvious to modify the disclosed watermark signals into cipher keys used for encryption. Sako provides motivation for this disclosure in the recitation, "The present invention provides a data recording device comprising a deciphering processing unit for deciphering and/or decompressing input

encrypted and/or compressed data by way of deciphering processing, a detection unit for detecting whether or not watermark signals are included in output data of the deciphering processing, a data processing unit supplied at least with data from the deciphering processing for applying signal processing for recording to the supplied data, a recording unit for recording output data from the processing unit on a recording medium, and a controller for controlling the operation of the data processing unit when the detection unit detects that the watermark signals are included, based on the so detected watermark signals (0010)." Besides that the Sako provides disclosure in Figure 1 of both an encryption circuit and deciphering circuit, which one of ordinary skill in the art could understand to handle encryption/enciphering and decryption/deciphering operations using the provided keys.

Although Sako is further silent in explicitly disclosing that the cipher key stored in cipher key memory unit is erased, the Examiner submits that it would have been obvious for one of ordinary skill in the art, at the time of the invention to have been motivated to combine the Sako and Montgomery references as the two references are directed toward the protection of valued information - data. Montgomery provides motivation and benefit of this combination as the key disclosed as being used in both references, is being used within the Montgomery reference as *an erasable*

key. Consider column 7 lines 12-21 of the newly included reference, Montgomery, which recites, "in one embodiment of the present invention, executing a tamper protocol (block 740) may erase the key to decode data stored in memory." Therefore, it would have been obvious to use an erasable cryptographic key, as claimed and argued by the Applicant, towards the protection of valued information – data, such as the copyright data of Sako.

Regarding claim 2, Sako et al., discloses the magnetic disk apparatus according to claim 1, wherein the cipher key memory unit stores a predefined cipher key written a stage of manufacturing the apparatus (0021-0024).

Regarding claim 3, Sako et al., discloses the magnetic disk apparatus according to claim 1, wherein the cipher key memory unit is a nonvolatile memory (0034).

Although Sako et al. does not explicitly disclose "nonvolatile memory," it would have been obvious to modify the disclosed recording medium memory – recording medium meaning a hard disc, an optical disc of the overwrite or write once type, a magneto-optical disc, magnetic disc, magnetic tape or IC card – into the "nonvolatile memory." In fact Examiner submits that the disclosed memory types are by definition

nonvolatile memory. Sako et al. provides motivation for this disclosure in the recitation, "When the second switching circuit 28 is off and the first switching circuit 27 is on, the encryption circuit 15 is supplied with compressed contents data deciphered by the deciphering circuit 12. The encryption circuit 15 encrypts compressed data, supplied thereto with cipher key data distinct from the cipher key data of the contents data supplied to e.g. the input terminal 11. The cipher key data is e.g. data based on a serial number etc. of the recording medium 16 on which to record the contents data. The encryption circuit 15 uses cipher key data distinct from the cipher key data used for the contents data supplied to the input terminal 11, or uses a distinct cipher system, to improve the safety of the contents data. The encryption circuit 15 outputs the encrypted contents data via second selector 22 to the recording processing circuit 19 (0028)."

Regarding claim 4, Sako et al., discloses the magnetic disk apparatus according to claim 1, wherein the cipher key memory unit is a medium area other than a user recording area of the magnetic disk medium (0023, 0028 and 0031-0034).

Regarding claim 6, Sako et al., discloses the magnetic disk apparatus according to claim 1, wherein the cipher key change unit replaces the cipher key in the

cipher key memory unit in response to a special command other than a command system for the upper apparatus (0027-0028).

Regarding claim 7, Sako et al., discloses the magnetic disk apparatus according to claim 1, wherein the cipher key change unit replaces the cipher key in the cipher key memory unit in response to a special command from a cipher key change application installed in the upper apparatus (0050-0052).

Regarding claim 8, Sako et al., discloses the magnetic disk apparatus according to claim 1, wherein the cipher key change unit replaces the cipher key in the cipher key memory unit in response to a special command from a cipher key change application installed by the upper apparatus via a network (0050-0052).

Regarding claim 9, Sako et al., discloses the magnetic disk apparatus according to claim 1, wherein the cipher key change unit replaces the cipher key in the cipher key memory unit by recognizing a physical event manipulation in the apparatus (0050-0052).

Regarding claim 10, Sako et al., discloses the magnetic disk apparatus according to claim 1, wherein the cipher key change unit replaces the cipher key by generating a new cipher key through a process of shuffling of the cipher key stored in the cipher key memory unit (0050-0052).

Regarding claim 11, Sako et al., discloses the magnetic disk apparatus according to claim 1, wherein the cipher key change unit replaces a cipher key stored in the cipher key memory unit into another cipher key added to a cipher key change command from the upper apparatus (0050-0052).

Regarding claim 12, Sako et al., discloses a cipher processing method for a magnetic disk apparatus, comprising: a cipher key memory step of storing in a stored in said cipher key memory unit, cipher key memory unit a single cipher key used for encoding and decoding data; an encoding/recording step of converting data input via an interface from an upper apparatus into encoded data using the cipher key, and recording the encoded data onto a magnetic disk medium; a decoding/readout step of decoding the encoded data read out from the magnetic disk medium using the cipher key stored in the cipher key memory unit, and outputting the decoded data via the interface to the upper apparatus; and a cipher key change step of erasing said cipher key stored in said cipher key memory unit, defined as a first cipher key with and replacing the first cipher key with another cipher key, defined as a second cipher key, which cannot decode the encoded data recorded on the magnetic disk medium; and wherein the cipher key change unit replaces the first cipher key stored in said cipher key memory unit with the second cipher key in response to a command for discarding all of a first encoded data recorded on the magnetic disk medium, and makes decoding

the first encoded data impossible, the first encoded data encodes using the first cipher key stored in said cipher key memory unit (Rejected under the same rationale as claim 1).

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully

consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHINWENDU C. OKORONKWO whose telephone number is (571)272-2662. The examiner can normally be reached on MWF 2:30 - 6:00, TR 9:00-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. C. O./
Examiner, Art Unit 2436

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436